

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
LUBBOCK DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

\$5,645,223.51 IN FUNDS SEIZED FROM
THE BANK OF AMERICA ACCOUNTS
WITH ACCOUNT NUMBERS ENDING IN
1133 AND 4983 HELD IN THE NAME OF
WIS SAFETY LLC

NO.

Defendant in rem.

COMPLAINT FOR FORFEITURE

Plaintiff, the United States of America files this verified complaint *in rem* against the defendant property, and states the following in support:

Jurisdiction and Venue

1. This court has subject matter jurisdiction of this cause of action *in rem* pursuant to 28 U.S.C. §§ 1345 and 1355(a). Venue is proper under 28 U.S.C. § 1355(b)(1) and 28 U.S.C. § 1395(b).

2. The statutory basis for this suit is 18 U.S.C. § 981(a)(1)(C). Also applicable are 28 U.S.C. §§ 2461 and 2465, 18 U.S.C. § 983, and 28 U.S.C. Rule G, Supplemental Rules for Admiralty and Maritime Claims and Asset Forfeiture Actions (Supplemental Rules).

The Defendant Property and its Location

3. The defendant property is comprised of \$5,645,223.51 seized from the Bank of America accounts with account numbers ending in 1133 and 4983 held in the name of WIS SAFETY LLC seized on or about October 14, 2020 by the United States Secret Service.

4. The defendant property is currently in the custody and management of the United States Secret Service (Department of Homeland Security) in the Northern District of Texas.

Legal Basis for Forfeiture

5. Title 18, United States Code, Section 1343, entitled “Fraud by Wire, Radio, or Television,” makes it a crime for anyone to use interstate or foreign wire communications in carrying out a scheme to defraud.

6. Title 18, United States Code, Section 981(a)(1)(C) provides that any property constituting or derived from proceed traceable to a violation of Section 1343 are subject to civil forfeiture.

Facts Supporting Forfeiture

7. A business email compromise is a type of computer-based fraud scheme. In this type of scheme, an individual “spoofs” the business email address of one employee at a company (or a legitimate vendor of the company) when sending an email to convince a second company employee to transfer company funds for a valid and legitimate company purpose, such as payment of a expense. In reality, however, the company funds have been “hijacked” by the individual sending the message using the

similar, but not identical business email address, usually into an account established solely to receive illegally-obtained funds.

8. Another recently-seen fraud scheme involves individuals fraudulently applying for and obtaining government loans using falsified, fraudulent, or stolen information of U.S. businesses. This type of scheme targets the Small Business Administration (“SBA”) Economic Injury Disaster Loan (“EIDL”) Program. In the scheme, an individual enters false, fraudulent, or stolen information into government-operated websites to attempt to obtain an EIDL; if the loan is approved, the loan funds are then sent via Automated Clearing House (“ACH”) transfer to a bank account specified by the applicant.

9. WSLLC had been established as a Limited Liability Company in Texas in 2016, but had forfeited its corporate charter in February 2020 and was no longer a viable business entity after that time.

10. In April 9, 2020, an application for an EIDL on behalf of WSLLC was received by the SBA. All personal and contact information listed on the application belonged to an individual named John Overman. The application claimed WSLLC’s gross revenue was \$120,000 over the past 12 months, stated that WSLLC had only one employee, and a JPMorgan Chase Bank account as the account into which to receive the loan. The loan was declined on May 23, 2020.

11. Subsequently, a business entity identified as Napier & Napier Farms (“N&NF”) applied for an EIDL. N&NF is purportedly located in Sioux Falls, South Dakota and has no identifiable ties to WSLLC. To date, N&NF has been involved with

over forty EIDL applications in which the loan beneficiary has been a third-party entity, not N&NF. The SBA-OIG and the USSS are currently investigating these loans.

12. On July 9, 2020, the Bank of America business checking account with account number ending in 1133 (“BOA1133”) and the Bank of America business checking account with account number ending in 4983 (“BOA4983”) were opened at a bank branch in Lubbock, Texas in the name of WIS SAFETY LLC (“WSLLC”). The sole signatory on the two accounts was John Overman, identified as WSLLC’s Managing Member. Overman resides in Brownfield, Texas.

13. On August 11, 2020, BOA4983 received an Automated Clearing House (ACH) payment for \$89,300.00 from the SBA. The payment’s source was an EIDL, with WSLLC as its beneficiary. However, the SBA loan number and customer identification connected to the \$89,300 payment belonged to N&NF, not WSLLC. Prior to the \$89,300.00 payment, BOA4983’s balance was \$100.00 (an opening deposit), and no other transaction had occurred with the account.

14. WSLLC was not authorized to receive an EIDL loan in August 2020.

15. On August 18, 2020, \$50,000.00 was transferred from BOA4983 to BOA1133. BOA4983’s balance then became \$39,400.00, and BOA1133’s balance became \$50,100.00.

16. Target Corporation is located in Minneapolis, Minnesota and does business with and regularly makes ACH payments to ICU Eyewear (“ICU”), a separate business that supplies eyewear to Target. Target conducts all of its accounts-payable transactions through Wells Fargo Bank’s Vendor Portal. Using the Vendor Portal, Target

vendors/suppliers have the ability to conduct business transactions with Target, as well as designate the respective bank accounts into which Target payments are received.

17. On or around August 7, 2020, ICU's designated account for receipt of Target payments in the Vendor Portal was altered to BOA1133. The change was enacted through the use of a "spoofed" ICU employee's email address; the address was similar, but not identical to, the employee's actual address, and the address had been substituted for an ICU employee's true email address. No ICU employee authorized or approved the change to ICU's bank account information in the Vendor Portal.

18. On August 19, 2020, and August 21, 2020, BOA1133 received two ACH payments – one for \$5,484,470.41, and the other for \$114,888.57 (\$5,599,358.98 in total). The payments were received from a Target-maintained Wells Fargo Bank account and were intended for ICU's benefit.

19. On August 19, 2020, \$43,481.00 was wired from BOA1133 to a Wells Fargo Bank account held by Tiejun Hu, a resident of Sugar Land, Texas.

20. On or around August 21, 2020, Bank of America froze the funds in both BOA1133 and BOA4983, after learning of the fraudulent transmission of the \$5,599,358.98 to BOA1133. As of September 17, 2020, the balance of BOA1133 was \$5,605,947.99, and the balance of BOA4983 was \$39,400.32. The United States Secret Service subsequently seized the funds in both accounts.

21. Overman contacted Bank of America employees on or around August 26, 2020, asking about the holds on BOA1133 and BOA4983. During that conversation, Overman stated that he was receiving the funds for a "hydroponic greenhouse." Though

bank employees asked Overman to provide documents to support his claims, Overman did not provide any materials indicating that he or WSLLC was authorized to receive the funds.

22. In summary, the defendant property was acquired through two criminal schemes, one in which individuals (unknown to date) illegally, and without authorization, caused the replacement of an ICU employee's email address with a similar, but slightly different email address, and then used the changed email address to effect, via additional wire communications, an unauthorized change to the bank account into which ICU would receive payments from Target. These individuals used electronic mail communications to change ICU's bank account information, and, as a result, the \$5,599,358.98 in ACH payments intended for ICU from Target were transmitted to BOA1133. In the other, an individual or individual made false, fraudulent, or misleading statements in an electronically-submitted EIDL application, resulting in \$89,300 being illegally transmitted to BOA4983. These two schemes violated 18 U.S.C. § 1343.

23. As of October 14, 2020, the funds on deposit in BOA1133 and BOA4983 constituted or are traceable to wire fraud proceeds. Pursuant to 18 U.S.C. § 981(a)(1)(C), these funds (up to \$5,688,658.98) are subject to seizure and forfeiture.

Relief Sought

24. Therefore, the United States requests the following:

- a. That the Clerk of Court issue a warrant for the arrest of the defendant property, pursuant to Rule G(3)(b)(i) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions;
- b. That the United States Marshals Service arrest the defendant property, pursuant to the warrant, as provided by Rule G(3)(c) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions;
- c. That the United States publish notice of the complaint for forfeiture on the website www.forfeiture.gov for at least 30 consecutive days, in accordance with Rule G(4)(a)(iv)(c) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions;
- d. That the United States deliver notice, pursuant to Rule G(4)(b) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions, to any person reasonably appearing to be a known potential claimant, advising the person of the date of notice; of the deadline for filing a claim; that an answer or motion under Rule 12(b) must be filed no later than 21 days after the filing of the claim; and of the name of the Assistant United States Attorney to be served with the claim and answer;
- e. That the court, after all proceedings are had on this complaint for forfeiture, declare the defendant property forfeited to the United States according to law;

f. That the court appropriately tax all costs and expenses incurred by the United States in obtaining the forfeiture of the defendant property against any persons or entities who filed a verified claim and answer in this case; and

g. That the court grant the United States any further relief, at law or in equity, to which it may show itself justly entitled.

Respectfully submitted,

PRERAK SHAH
ACTING UNITED STATES ATTORNEY


/s/ John J. de la Garza
JOHN J. DE LA GARZA III
Assistant United States Attorney
Texas Bar No. 00796455
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Tel: 214.659.8682; Fax: 214.659.8803
Email: john.delagarza@usdoj.gov

Verification

I am a Special Agent with the United States Secret Service. As an Agent with the USSS, my duties and responsibilities include participating in the investigation and prosecution of persons who violate federal laws.

I have read the contents of the foregoing Complaint for Forfeiture and verify under penalty of perjury pursuant to 28 U.S.C. § 1746 that the factual statements contained therein are true and correct to the best of my knowledge and belief.

Executed on this 7 day of April, 2021.

A handwritten signature in black ink, appearing to read 'P. Hooton', is written over a horizontal line.

Patrick Hooton, Special Agent
United States Secret Service